

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

Plaintiff,

v.

Case No. 1:22-cv-00187

SKYRYSE, INC., ROBERT ALIN PILKINGTON,
MISOOK KIM, and DOES NOS. 1-50,

Defendants.

**PLAINTIFF’S OPPOSITION TO DEFENDANT SKYRYSE, INC.’S
MOTION TO ENTER SOURCE CODE PROTOCOL**

TABLE OF CONTENTS

	Page
PRELIMINARY STATEMENT	1
POINT I. MOOG MUST BE ABLE TO COMPARE ITS CODE WITH SKYRYSE’S CODE ON THE SAME DEVICE USING COMPARISON TOOLS.....	3
POINT II. THE COURT’S INSPECTION PROTOCOL IS SAFE, SECURE AND EFFICIENT.....	4
A. The Use of the Parties’ Agreed Third-Party Neutral, iDS, Does Not Merit a Separate Protocol	5
B. There Are No “Internet Access” Security Problems.....	6
C. Skyryse’s Purported Concerns About Printing Source Code Are Baseless.....	7
D. The Court’s Inspection Protocol Has Substantial Safeguards Regarding Copying Source Code	10
POINT III. SKYRYSE’S SECOND PROTOCOL IS UNPRECEDENTED, NOT THE EXISTING INSPECTION PROTOCOL.....	10
A. Other Courts Have Allowed Side-by-Side Code Comparison.....	10
B. Skyryse’s Cited Authority is Distinguishable.....	13
POINT IV. SKYRYSE HAS COPIED MOOG’S CODE, NOT THE REVERSE	15
POINT V. THE COURT’S INSPECTION PROTOCOL’S APPLICABILITY IS NOT LIMITED TO ONLY CERTAIN SOURCE CODE	16
CONCLUSION.....	17

TABLE OF AUTHORITIES**Page****Federal Cases**

<i>AMO Development, LLC v. Alcon LenSx, Inc.</i> , C.A. No. 20-842 (D. Del.)	9, 11, 12
<i>Crawford-El v. Britton</i> , 523 U.S. 574 (1998).....	17
<i>ImageKeeper LLC v. Wright National Flood Insurance Services LLC</i> , 2:20-cv-01470-GMN-VCF (D. Nev. 2021)	13
<i>SMH Enterprises, L.L.C. v. Krispy Krunchy Foods</i> , Case No. 20-cv-02970 (E.D. La. 2020)	11
<i>Softketeers, Inc. v. Regal West Corporation</i> , 8:19-cv-00519-JVS (C.D. Cal. 2020)	5
<i>Syntel Sterling Best Shores Mauritius Limited v. The Trizetto Group, Inc.</i> , C.A. No. 15-00211 (S.D.N.Y. 2016)	12

Federal Statutes

18 U.S.C. § 1839(3)(A).....	12
18 U.S.C. § 1839(5)(B).....	11, 12

PRELIMINARY STATEMENT

Skyryse's second source code protocol apparently has one chief goal—to hobble Moog's ability to conduct an effective comparison of the parties' source code. This is demonstrated and confirmed by Section 4.3(c) of Skyryse's proposed additional source code inspection protocol, which would only permit Moog's experts to bring its source code into the physical room on paper or a separate computer. The parties' source code would not be available on the same computer. As explained by Moog's expert, Kevin Crozier (who has years of experience conducting audits of flight control software), this would cripple his ability to conduct an effective source code comparison. This is because Skyryse's proposed process would require a *manual* comparison of the parties' code—for example, for him to look at a page of Moog's code (on paper or on a computer), then look at a page Skyryse's code (on a separate computer), and determine from eyeballing the two whether there are similarities or differences. This makes no sense when roughly 43,000 files of Moog's source code (by our current estimate) were stolen by Skyryse and can potentially be found in Skyryse's code. Such a process would also cause substantial delays and be far more prone to error. Conversely, under the Court's Inspection Protocol, which facilitates having both parties' code available on the same computer, Moog's expert can use software tools for efficient and accurate analysis and comparison.

Skyryse even goes so far as to claim that no comparison is needed, as its source code at issue does not contain any Moog information. This claim cannot be taken at face value. Moog must be permitted to test those representations, especially given that Moog has *already* found evidence of Skyryse directly copying Moog's source code. A comparison of the source code both parties have produced through iDS has already revealed dozens of examples of direct copying by Skyryse.

Skyryse’s purported “security” concerns regarding the Court’s Inspection Protocol are specious. The use of iDS does not by itself create any security problems. The parties *jointly* selected iDS. Specifically, Skyryse agreed to iDS after performing its own diligence and rejecting several other companies proposed by Moog. The Parties have already relied on iDS to make source code available, and Skyryse does not point to any example of how its code has not been handled securely. There are no “internet access” issues, as reviewers literally have no ability to access or transmit any inspection materials over the internet from iDS computers. And the “internet browsers” are completely irrelevant to security. The only reason why internet browsers like Chrome are available on the iDS virtual machines is because they are needed to view HTML files turned over by Skyryse. Nobody can access the internet using the internet browsers. And, contrary to Skyryse’s representations, the Inspection Protocol expressly prohibits the copying of any Inspection Materials (including source code).

Finally, Skyryse’s claim that source code printing limits must be implemented is baseless. The Inspection Protocol already contains detailed procedures for requesting the printing of code, and for the producing party to object to those requests before raising it with the Court. Skyryse’s proposal for a 100-page printing limit is completely nonsensical in a case where roughly 43,000 source code files were stolen. By way of example, just 24 of the Skyryse source code files that Moog has already identified as being direct copies of Moog code constitute almost 300 pages by itself.

The Court’s Inspection Protocol is extremely secure and robust, and has already been used for source code production, inspection, comparison, and analysis. The Court should deny Skyryse’s motion to enter a second source code inspection protocol.

POINT I. MOOG MUST BE ABLE TO COMPARE ITS CODE WITH SKYRYSE'S CODE ON THE SAME DEVICE USING COMPARISON TOOLS

Moog's evaluation of trade secret theft and use requires direct comparison of files, which is only practicable under the Inspection Protocol because both parties' files are housed on the same machine. Skyryse has already admitted that it has produced voluminous source code files through iDS under the Inspection Protocol. Moog has already produced relevant source code through iDS. Skyryse's experts have been reviewing materials on iDS devices for weeks, so it is reasonable to infer that they have already accessed and reviewed Moog's source code. If Skyryse's second inspection protocol were to be entered, there would be two separate protocols for reviewing two separate groups of Skyryse source code.

In its Motion, Skyryse says section 4.3(c) of its proposed protocol would permit Moog to bring copies of its own source code, either as a printout or on a separate secured computer, into Skyryse's physical inspection room. (ECF 213-002 at pp. 7-8). However, this is insufficient. Both Moog's and Skyryse's code need to be available *on the same computer* so that source comparison tools can be used. (Declaration of Kevin Crozier ("Crozier Dec."), ¶ 15). Without the ability to use source comparison tools, Moog's experts would be forced to perform manual comparisons. (*Id.*, ¶ 16). This will be very slow and error-prone since Moog's experts will have to look between two different computers (or between printouts of code and a computer) and then manually identify the similarities and differences. (*Id.*). Given the volume of Moog's source code files that were stolen (roughly 43,000 by our current estimate), a manual comparison is impracticable, inefficient, and improper for the needs of this case. (*Id.*). And given that this Court's trade secret identification order provides that Moog must further identify its trade secrets after a "reasonable (but not too long) time" (ECF 205 at p. 3), Moog's trade secret identification

process would be delayed significantly if its experts were only permitted to perform a manual comparison.

We believe that Skyryse’s goal through a second separate protocol is to hobble Moog’s ability to effectively conduct further source code comparison, because Moog’s inspection to date *has already revealed dozens of examples of direct copying by Skyryse*. (ECF 210 at pp. 4-5). Skyryse argues that Moog has “made no showing that the Skyryse code at issue ‘necessarily includes’ anything belonging to Moog.” (Mot at p. 10). But Moog is entitled to test that self-serving claim.¹

POINT II. THE COURT’S INSPECTION PROTOCOL IS SAFE, SECURE AND EFFICIENT

The Court’s Inspection Protocol sets up a robust security mechanism through the neutral forensic vendor iDS for remote review. (Declaration of Bruce W. Pixley (“Pixley Dec.”), ¶ 9). Only iDS—and none of the parties—have possession of the source code for inspection. (*Id.*). All of the source code is housed on iDS’s central servers (virtual machines) not on any local laptops in the possession of any parties or reviewers. (*Id.*). In other words, the source code never leaves iDS premises. While the reviewers access iDS’s virtual machines using laptops, those laptops contain zero source code. (*Id.*). No one can access the virtual machines without presenting government-issued ID to an iDS inspection supervisor via the webcam on the laptops

¹ Skyryse may offer in reply to let Moog bring all of its source code on an external hard drive (like a USB drive) and plug it into Skyryse’s physical computer in the physical inspection room, so that both parties’ code can be compared on the same computer. This would not be acceptable. There is no reason for Moog to risk the security of its source code by plugging all of it onto its *adversary’s* computer (an adversary who has already admitted to theft of over 1.4 million of its files). That is what a neutral like iDS is for—so that neither Moog nor Skyryse has to do this. If both parties’ source code will be put on a single computer for side-by-side inspection, it should be iDS’s computer, not Skyryse’s.

and the entire visual stream of the inspection is videorecorded. (*Id.*). The Inspection Protocol also details who can receive source code materials, and how they are to be transmitted, stored and used. (ECF 96-02, §§ I.1 and VIII). As this Court noted, “the measures which Moog proposes adequately address [Skyryse’s] concerns” regarding “potential disclosure of its own privileged and/or confidential information.” (ECF 109 at p. 2).

The inspection of source code under the Inspection Protocol is also practical, efficient, and safe, because it is remote. It minimizes, or even eliminates, in-person contact—a very important consideration as we are still in the midst of a pandemic. Indeed, courts have fashioned source code protocols to allow for remote inspection in light of travel and health concerns because of the ongoing pandemic. *See Softketeers, Inc. v. Regal West Corporation*, Order Granting Stipulated Motion for Altered Source Code Review Procedures in Light of U.S. Pandemic Response, 8:19-cv-00519-JVS (C.D. Cal. 2020), ECF No. 427 (allowing source code held by a neutral third party to be downloaded to provided laptops of each party’s source code expert). (Declaration of Rena Andoh, Ex. A).

Meanwhile, Skyryse’s Motion identifies four purported problems with the Court’s Inspection Protocol: (1) the use of a third party, i.e., iDS ; (2) purported “internet access” security issues; (3) the purported need for source code printing limits; and (4) the purported risk of copying of source code. (Mot. at pp. 3-6). As explained below, all of these grounds lack merit.

A. The Use of the Parties’ Agreed Third-Party Neutral, iDS, Does Not Merit a Separate Protocol

Skyryse generally claims that the Court’s Inspection Protocol “provides a complex, intricate procedure reliant entirely on a third party.” (Mot. at p. 3). But these are

exactly the procedures that ensure the security of all parties’ confidential data (and no doubt if the “complex, intricate procedures” were absent Skyryse would be complaining about the lack of security). Skyryse also generally complains that the “very involvement and reliance on a third-party vendor complicates the process and makes it more expensive” (*id.* at p. 4). But clearly that cost has already been and will continue to be incurred no matter what (for the millions of files that have already been turned over), and adding a second protocol will not make that cost go away. To the contrary, adding a *second* protocol will only compound the cost. Skyryse also argues that turning over each party’s source code to iDS would cause the parties to “effectively lose the ability to monitor and supervise its distribution.” (*Id.* at p. 4). But that’s what iDS is for—to monitor and supervise the inspection—as they have been doing, and Skyryse has not identified anything deficient about that process.

B. There Are No “Internet Access” Security Problems

Skyryse complains that the Court’s Inspection Protocol “unquestionably allows for internet access” and that “Moog has already installed standard web browsers, through which one could make source code available over the Internet.” (Mot. at pp. 4-5). This is simply false and misrepresents the Court’s Inspection Protocol.

Each Inspection laptop, which was configured and locked down by iDS per the Court’s Inspection Protocol, is limited to two applications that can be used by a reviewer: Microsoft Remote Desktop and Zoom. (Pixley Dec., ¶ 12). The Microsoft Remote Desktop application is configured to connect to specific Remote Desktop sessions (“Remote Session”) hosted by iDS. (*Id.*, ¶ 11). The Remote Sessions do not allow outside internet access as outside internet access has been strictly blocked by iDS. (*Id.*, ¶ 13). While a Remote Session may have a

web browser installed, a reviewer cannot access internet-based content. (*Id.*). This includes a complete restriction on access to web sites, print services, cloud storage, email, chat communications, and file transfer services. (*Id.*). The one and only method for a reviewer to export content from the Remote Session is pursuant to the Court’s Inspection Protocol, Section III.F.2. Under this provision, a reviewer’s privileged notes can be exported by iDS, but only after a request that is copied to all parties. (*Id.*, ¶ 15; ECF 96-2, § III.F.2). That a reviewer can have iDS export his privileged notes out of the Remote Session is no different-in-concept than a reviewer being able to take his paper notes out of a physical inspection room after an inspection.

Notably, Moog has had access to certain Skyryse devices via iDS for over 7 weeks now, and Skyryse does not identify a single instance where security protocols in the Court’s Inspection Protocol have proven inadequate. Skyryse also does not identify any instance where Moog improperly used internet access, or transmitted Skyryse information over the internet (as this is impossible to do under the Inspection Protocol). (*Id.*, ¶ 17). Skyryse’s specious security “concerns” do not justify the unprecedented step of instituting a second source code protocol.

C. Skyryse’s Purported Concerns About Printing Source Code Are Baseless

Skyryse argues “nothing would prevent someone under the iDS Protocol from printing out an adversary’s *entire codebase* and taking it to an unsecure location, undermining the whole purpose of a restrictive review process.” (Mot. at p. 5). This is false. The Court’s Inspection Protocol already has robust procedures for requesting, and objecting to, the production of source code. Specifically, the Court’s Inspection Protocol provides that the “Receiving Party may request production of documentary Inspection Materials” but that “[i]f the

Producing Party objects to production of Inspection Materials, the parties must promptly meet and confer.” (ECF 96-02 at §§ IV.1 & IV.3, pp. 12–13). If the parties cannot agree, then the Producing Party can prevent the production by filing a request with the Court within five business days of the meet and confer, and then the Court will decide. (*Id.* at § IV.3, p. 13). Moreover, the Inspection Protocol has a provision that expressly prohibits abuse of the requests for production of source code, as follows:

The Receiving Party shall not request production of Source Code in order to review Source Code outside of the Inspection Laptop in the first instance, as the parties acknowledge and agree that the purpose of the protections herein would be frustrated by such a request. Production of Source Code is permitted solely to enable use of such Source Code in filings, depositions, proceedings, contentions, expert reports, and related drafts and correspondence.

The Inspection Protocol has detailed provisions in place regarding printing of source code, requires meet and confer to the extent there are any disputes, and prohibits abuse of production of source code. If Moog requests the production of Skyryse’s entire codebase, for example, Skyryse can object to that request and seek relief from the Court. Notably, Skyryse does not and cannot point to any example where Moog has abused the Inspection Protocol regarding the requesting printing of source code. Indeed, it is Skyryse who has not produced a single document that Moog has requested pursuant to the Court’s Inspection Protocol. (*See* ECF 226).

Skyryse claims there must be “reasonable limits on the printing of code” and proposes a printing limit on consecutive pages (10) and total pages (100) that may be requested. (*Id.*). No such limits are necessary because the Court’s Inspection Protocol already has robust procedures for objecting to production of source code, as explained above. But even if the Court were to find that presumptive limits are appropriate, Skyryse’s proposed printing limits are inappropriate for a case involving the theft of roughly 43,000 source code files (by our current

estimate). Notably, as an example reflected in Moog's recently filed Motion to Compel, Moog's experts identified via iDS 24 Skyryse source code files that are identical or near-identical copies of 24 Moog source code files. (ECF 210 at pp. 4-5). The number of pages just involved in those 24 source code files *is approximately 20,000 lines of code, or approximately 300 pages*. (Crozier Dec., ¶ 13). This is just one example out of many of the groups of code that Moog will need to be printed to put in front of the Court via expert reports or other motion practice.

For example, in *AMO Development, LLC v. Alcon LenSx, Inc.*, C.A. No. 20-842 (D. Del.), there was no aggregate limit on source code printing, and there was a limit of 2,500 pages of source code printing at any one time. (ECF 211-006 at pp. 16, 48). And there were no allegations in the *AMO* case of theft of over 1.4 million files, of which roughly 43,000 were source code files. A 100-page limit is simply not appropriate or congruent with the scale of trade secret theft at issue.

Further, the Court's Inspection Protocol need not contain specific security restrictions on storage of printouts of source code because the Protective Order already places very secure limits on how the Parties are to treat designated material. (ECF 89). Notably, software design documents, software requirements documents, and software checklists are extremely valuable in the aviation/FAA context. (Crozier Dec. ¶¶ 17-21). These non-code documents do not get any special storage treatment under the Inspection Protocol, but are instead protected by the Protective Order just as all source code would be.

D. The Court’s Inspection Protocol Has Substantial Safeguards Regarding Copying Source Code

Skyryse claims that only its proposed protocol “prohibits reviewers from copying source code into their notes.” (Mot. at p. 6). Skyryse acknowledges that the Inspection Protocol prevents the use of notes “to recreate the materials for outside use,” but then vaguely claims it “creates unnecessary risk for sensitive source code.” (*Id.*). Even though Moog has had access to certain Skyryse devices via iDS for over 7 weeks, Skyryse does not and cannot point to any example where a party has copied code or other documents. And, again, Skyryse blatantly misrepresents the actual provisions of the Inspection Protocol.

Section III.H.1 of the Inspection Protocol states, in no unambiguous language, that:

the Receiving Party shall not email, upload, download, copy, or electronically transmit or electronically store any Inspection Materials from the Inspection Laptop *(including but not limited to, through use of a camera or imaging device). The Inspection Laptop shall not be connected to a printer in any way.*

(ECF 96-02 at p. 12 (emphasis added)). So, Skyryse’s claim that only its proposed protocol “prohibits reviewers from copying source code into their notes” is false. The Inspection Protocol expressly prohibits any copying.

POINT III. SKYRYSE’S SECOND PROTOCOL IS UNPRECEDENTED, NOT THE EXISTING INSPECTION PROTOCOL

A. Other Courts Have Allowed Side-by-Side Code Comparison

Skyryse’s claims the Inspection Protocol entered by the Court is “unprecedented.” (Mot. at p. 6). This is simply incorrect. As requested by the Court, on August 3 Moog submitted

a letter brief with cases where parties produced their source code to a third-party vendor which permitted side-by-side code comparison. (ECF 211).

For example, in *SMH Enterprises, L.L.C. v. Krispy Krunchy Foods*, Case No. 20-cv-02970 (E.D. La. 2020), the parties were subject to a protective order requiring the parties to produce their respective source code to a third party escrow agent for hosting. (ECF 211-004 at p. 10). The protocol required that the third party only provide access to a limited subset of people, including the attorneys, experts, and any Court-appointed special masters. (*Id.*). Here, the parties produced source code to iDS, and iDS preconfigured inspection laptops for a limited number of reviewers to access the virtual machines that store the source code.

In its August 10 letter brief, Skyrise attempts to distinguish *SMH*, which is directly on point, by claiming that the “protective order does not contemplate or provide any means for a side-by-side comparison.” (ECF 224 at p. 4). But, the protective order at issue states that “[a]ny source code produced by a party . . . shall be delivered to a qualified third party which Escrow Agent shall provide access only to the Parties’ attorneys . . . expert witnesses . . . and Court-appointed special master(s).” (ECF 211-004, § 11(h)). There is nothing in this provision that prohibits side-by-side comparison, and the language of the order makes clear that the parties’ counsel will get full access to all source code produced. There is no language whatsoever requiring that source code be placed on a standalone machine requiring physical inspection .

In the August 10 letter brief, Skyrise also attempts to distinguish *AMO*, a case cited by Moog, by arguing that is a copyright case and that copyright claims use the “substantial similarity” test, whereas trade secrets rely on a different test. This argument fails as a matter of law and common sense. Misappropriation of a trade secret includes “use” of a trade secret. 18

U.S.C. § 1839(5)(B). If a defendant has verbatim copied the plaintiff’s source code (as Skyryse has here) such that it is “substantially similar” under a copyright infringement test, then that clearly also supports evidence of “use” under a trade secret misappropriation test. Whether *other* aspects of the trade secret misappropriation test are satisfied (e.g., whether the plaintiff kept the information secret, 18 U.S.C. § 1839(3)(A)) are separate issues.

Skyryse also attempts to distinguish Moog’s reliance on *Brocade*, arguing that there were multiple causes of action there (copyright, trade secret, and patent claims) and the source code comparison was used in that case only for the copyright claims. (ECF 225 at p. 4). For the same reason identified above for *AMO*, the argument that a finding of “substantial similarity” between the parties’ source code would not support a trade secret claim fails as a matter of law. There can be no doubt that, as a practical matter, the plaintiff in *Brocade* used its findings during the source code comparison to support its claims of trade secret misappropriation, regardless of what labels were placed on the inspection. But the plaintiff in *Brocade* was permitted to find *other* evidence of trade secret misappropriation during the “subsequent” phases of inspection, e.g., “use” under 18 U.S.C. § 1839(5)(B) that goes beyond copying. In any event, there are other cases with both copyright and trade secret claims where the court allowed full comparison of source code for both sets of claims. *See Syntel Sterling Best Shores Mauritius Limited v. The Trizetto Group, Inc.*, Stipulated Protective Order at §36.g, C.A. No. 15-00211 (S.D.N.Y. 2016), ECF No. 207 (in a case with copyright and trade secret claims, the protective order specifically allowed a source code laptop to be connected to another stand-alone computer for “the sole purpose of comparing source code.”). (Andoh Dec., Ex. B).

Also, as Moog explained in its letter, one of the reasons it cited *Brocade* was to show how a case venued in the Northern District of California, with its own default “Model Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets” that Skyryse suggests this Court adopt, still elected to fashion its own protocol tailored to the unique needs of that case. Similarly here, the Court’s Inspection Protocol allows for the Court to tailor an inspection procedure that is appropriate for our case dealing with at least 1.4 million stolen files and reviewing them safely in a pandemic.

There are other examples of Courts requiring trade secret litigants to produce source code to a third party. For example, in *ImageKeeper LLC v. Wright National Flood Insurance Services LLC*, the parties stipulated to a protective order requiring a “remote reviewing system” using a “third-party equivalent secure source code review solution.” Stipulated Protective Order at §9.a, 2:20-cv-01470-GMN-VCF (D. Nev. 2021), ECF No. 148. (Andoh Dec., Ex. C). Among other similarities to this Court’s Inspection Protocol, *ImageKeeper*’s protocol required a two day notice of which reviewer will be accessing the remote reviewing system to allow for live monitoring of the inspection. *Id.*

By contrast, Skyryse does not and cannot cite a single case where a court entered a *second* source code inspection protocol under circumstances similar to those before this Court.

B. Skyryse’s Cited Authority is Distinguishable

Skyryse cites to eight cases to argue that its source code protocol “is modeled after standard source code review protocols routinely entered in trade secret cases across the country.” (ECF 213-1 at p. 6). However, this argument ignores the Court’s Inspection Protocol currently in effect, which is tailored to our unique case involving the theft of over 1.4 million

files taken from Moog during the COVID-19 pandemic. Skyrise's source code protocol is not only unnecessary with the Court's Inspection Protocol, but it will also create unnecessary confusion if implemented. In addition, the eight orders and stipulations Skyrise cites to, which include language regarding source code review, are highly distinguishable for several further reasons.

First, all of the cited cases only involve one source code review protocol, unlike here, where Skyrise is trying to add a second different and separate protocol to address the review and production of two different groups of source code, in addition to the Court's Inspection Protocol that already governs the review of source code via iDS.

Second, in all of these cases, the parties did not have a third party neutral vendor involved for the purpose of safely producing and reviewing source code. Here, the parties have already involved iDS in conjunction with the Court's Inspection Protocol to provide an extremely secure and robust security mechanism for remote review, which is especially relevant during a pandemic. Third, in all of these cases, source code was made available on a stand-alone computer (i.e., not linked to or accessible from any network) located at the office of one of the parties' law firms, which would create unnecessary in-person contact during a pandemic. Here, the restricted inspection laptops, pre-configured by iDS to allow for remote inspection, are networked in order to remotely access the virtual machines where the relevant files are located. However, other than this network connection allowing access to the virtual machines, which are in the custody of the third party neutral vendor, "[e]ach Inspection Laptop [is] restricted such that there is no internet access beyond the domains necessary for remote access to the Inspection

Materials, use of any review or inspection tools, and videoconference monitoring services.”
(ECF 96-2 at p. 6).

Finally, there is no indication in any of these cases that any party had already produced substantial source code before the order or stipulation at issue was entered into. Here, Skyryse has already produced source code repositories and other volumes of source code to iDS and has produced to Moog at least 295 files designated as source code covering 2,186 pages. Therefore, Skyryse’s reliance upon these cases is misplaced.

POINT IV. SKYRYSE HAS COPIED MOOG’S CODE, NOT THE REVERSE

Skyryse claims that a separate source code protocol is needed because Moog will “root around in Skyryse’s code” for “any similarities to Moog’s code” to “spin as ‘trade secrets’ or “take credit for Skyryse’s innovations” (Mot. at pp. 10-11). Not only is such a suggestion lacking in any support, but it is incredible for Skyryse to suggest Moog will misuse Skyryse’s code given the events that have transpired in this case.

It is confusing that Skyryse would point the finger at Moog when Moog has already demonstrated to this Court *multiple examples of Skyryse copying, word for word, Moog’s source code and other software documents*. (ECF 210 at pp. 4-5). This is on top of the admitted theft of over 1.4 million files by former Skyryse employees, Skyryse’s admitted possession of large volumes of Moog confidential information, and Skyryse’s admitted spoliation of relevant evidence. Moog has not abused the existing Inspection Protocol in any way, and Skyryse does not point to any such example. If any party has legitimate concerns about someone else “taking credit” for its “innovations,” it is Moog.

Finally, Skyryse’s suggestion that Moog’s production of its source code to iDS was made so that it could get “virtually unfettered access to Skyryse’s code” is baseless and improper. (Mot at p. 10). Moog and Skyryse both produced their respective devices containing source code to iDS for the same reasons: so that the information would not be produced directly to the other side in the first instance. The Parties agreed, as part of the March 11 Order, to have a neutral forensic firm handle these and other aspects of discovery in this case. Skyryse’s attempts to draw nefarious motives from Moog making its source code available for review (in the same manner that Skyryse already has) is unfortunate.

**POINT V. THE COURT’S INSPECTION PROTOCOL’S
APPLICABILITY IS NOT LIMITED TO ONLY CERTAIN
SOURCE CODE**

There is nothing in the Court’s inspection protocol that limits it to documents turned over pursuant to the March 11 Order. Instead, it covers materials “made available for inspection through neutral forensic vendor iDiscovery,” i.e., iDS. (ECF 96-2, p. 1). There is no reason why Skyryse cannot make all of its source code available for inspection through iDS, as both Moog and Skyryse have *already* done for collectively tens of thousands of source code files.

Skyryse’s mischaracterization of the Inspection Protocol (including its purported security deficiencies) is highlighted by the fact that Skyryse acknowledges that “portions of Skyryse source code” are already “available for [Moog] to inspect under the iDS Protocol.” (Mot. at p. 9). Skyryse also claims that a second protocol is needed because the protective order entered by the Court “expressly contemplates that the [parties] would negotiate another stipulation to govern the review of their confidential source code.” (Mot., p. 3). But that is

exactly what happened here. After the Parties met and conferred and could not reach agreement, the Inspection Protocol entered by the Court on May 13 is titled “ADDENDUM TO PROTECTIVE ORDER” and expressly states in the first paragraph that it is intended to, among other things, cover “Source Code.” (ECF 96-02, p. 1).

Judicial economy, efficiency, and practicality would be served by requiring all source code production and review to take place under the Court’s Inspection Protocol, remotely through iDS, especially given that Moog and Skyryse have *already* produced large volumes of source code to iDS. *See Crawford-El v. Britton*, 523 U.S. 574, 599 (1998) (“the discovery process [should] facilitate prompt and efficient resolution of the lawsuit.”).

CONCLUSION

Moog respectfully requests that the Court deny Skyryse’s Motion in full, and order Skyryse to produce all of its source code responsive to Moog’s Interrogatory No. 1 to iDS pursuant to the existing Inspection Protocol within 7 days.

Dated: New York, New York
August 17, 2022

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
Attorneys for Plaintiff Moog Inc.

By: s/Rena Andoh
Rena Andoh
Travis J. Anderson (admitted *pro hac vice*)
Lai Yip (admitted *pro hac vice*)
Tyler E. Baker (admitted *pro hac vice*)
Kazim A. Naqvi (admitted *pro hac vice*)
30 Rockefeller Plaza
New York, New York 10112
(212) 653-8700

and

HODGSON RUSS LLP

By: s/Robert J. Fluskey, Jr.

Robert J. Fluskey, Jr.

Melissa N. Subjeck

Reetuparna Dutta

Pauline T. Muto

The Guaranty Building

140 Pearl Street, Suite 100

Buffalo, New York 14202

(716) 856-4000